音声 Vibe Coding における日本語音声の誤認識と AI 補正がセキュリティに及ぼす影響

崎山・李・宮原研究室

Vibe Coding とは

Vibe Coding とは、開発者が自然言語で指示を出し AI にコードを生成させる新たな開発手法である。近年では、作業効率を上げるために**音声による Vibe Coding** が急速に普及しつつある。

AI 音声整形ツール「Typeless」について

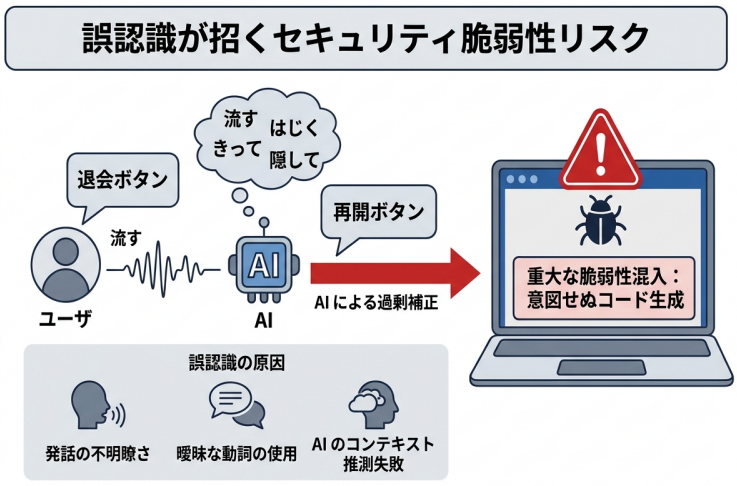
音声入力特有の言い淀みなどを検知し、文脈から**自然なテキストへ自動整形**する AI ツール。本研究では、この「文脈からの推測」がコードの正確性に及ぼす影響を検証する。

Typeless
Your voice is the new keyboard

AI 自動整形の危険性とセキュリティリスク

実験の結果、AI の**過剰補正による誤変換**や意図せぬコード改変などの**脆弱性混入リスク**が確認された。

- **意図せぬ変換:** 「退会」が「再開」に変換されるなど、正反対の処理となるケースが発生。
- **セキュリティへの影響:** 文法的には自然なため開発者が見落としやすく、致命的なバグに繋がる危険性がある。



制作者: 山本 怜奈

崎山・李・宮原研究室 HP: https://sakiyama-lab.jp/